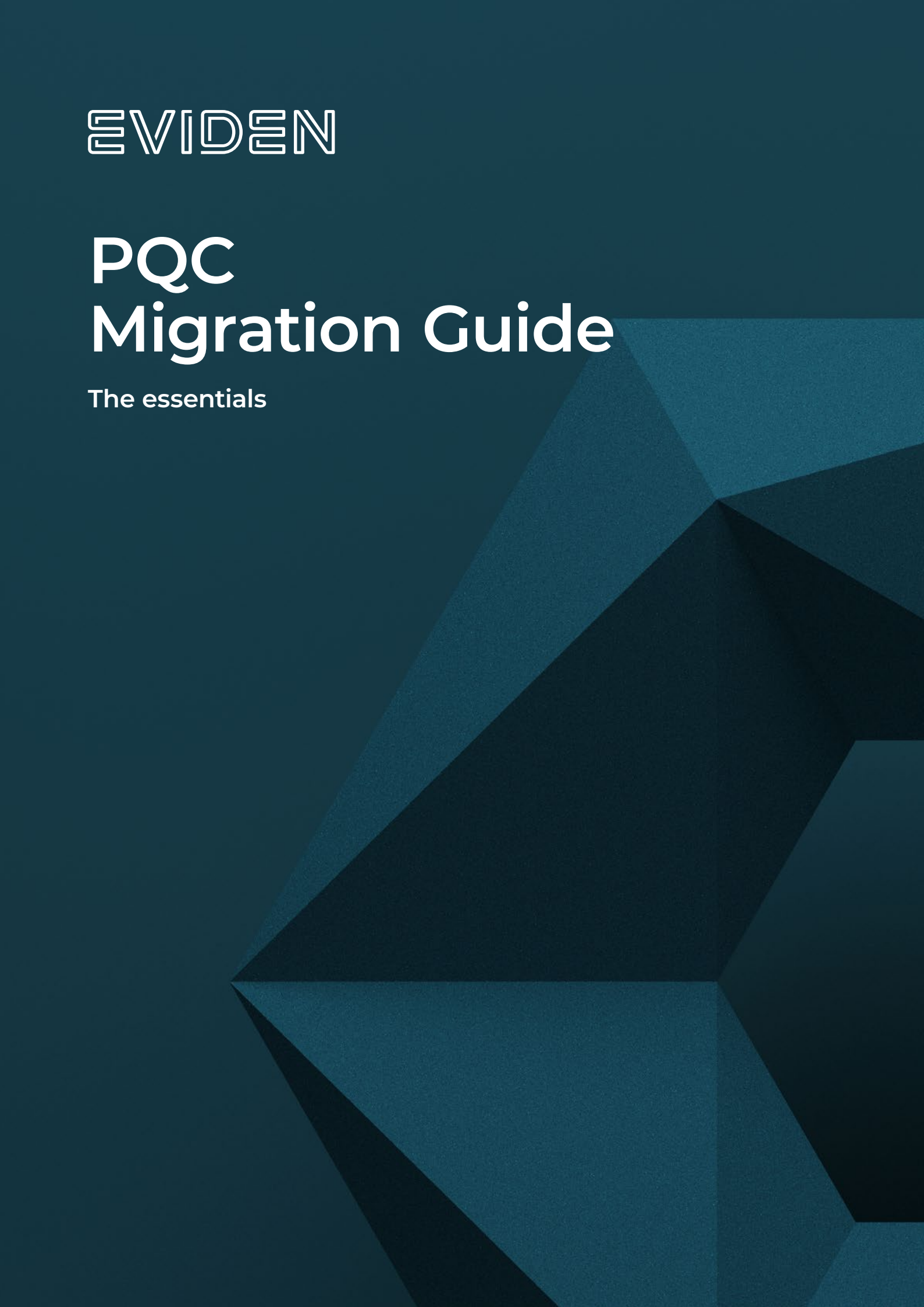
EVIDEN

PQC Migration Guide

The essentials



Contents

Management summary

Does the notion of a hacker penetrating your corporate network and reading your encrypted emails while accessing your company's most sensitive data disturb you? This scenario is more realistic than one might think, especially when cryptographically relevant quantum computers will be available. At that point all crypto systems based on RSA, Diffie-Hellman, or ECC could be easily attacked. These cryptographic mechanisms represent the current security bedrock and are used billions of times in web browsers, e-mail clients, smartphones, VPN solutions and operating systems.

Fortunately, we have not reached the brink where current systems are vulnerable. While quantum computers already exist, current models are far too weak and noisy to break any real cryptographic system just yet. But the technology is significantly progressing and therefore quantum-resistant alternatives must be developed. Such "post-quantum cryptography" (PQC) methods already exist. After years of academic research, some of these are now ready for standardization. CRYTSTALS Kyber (key exchange) and CRYSTALS-Dilithium (digital signatures) are the techniques you may have heard of.

The migration to post-quantum cryptography represents one of the most significant challenges in IT and will be major task for the years to come for everyone from for protocol designers, cryptography vendors and every virtually all members of an organization's IT infrastructure.

One obvious challenge is that post-quantum methods require more computing resources than the currently utilized RSA, Diffie-Hellman, and ECC schemes. Proposed PQC methods use public/private key lengths significantly larger than current key lengths while the overall performance is lower. This can be especially challenging for using existing tokens like smart cards for secure storage of private key date as these limited resource environments are not designed to support algorithms with the characteristics that PQC is based upon.

Because the currently proposed post-quantum cryptographic algorithms are not as mature than their conventional counterparts, most experts agree that more analysis is needed as the potential for a vulnerability is greater than thoroughly tested systems. Thus the need for crypto agility, the ability to rapidly transition to an alternative standard without making significant changes to the environment is quite significant. Organizations that will be able to implement changes between cryptographic algorithms in running systems will be best prepared for the risks of a particular standard being broken in the future.

Migration strategies where one shuts down all classic cryptographic systems and restarts them with post-quantum algorithms are simply not realistic. Therefore, it is recommended to plan a phased migration project that may include hybrid methods where a combination of pre- and post-quantum algorithms are dually used for a transition phase. By following the steps exposed in this paper, you will be better prepared for such a project. The first step of post-quantum migration should always be the generation of a crypto inventory. The systems listed in such an inventory need to be classified and prioritized.

As an expert in the field of quantum computers as well as in cryptography. Eviden is your ideal partner when it comes to post-quantum cryptography. Our cryptographic products, including Hardware Security Modules (HSMs), email encryption software, VPN solutions, PKI systems and Identity & Access Management (IAM) solutions, are currently made quantum-proof. In addition, we at Eviden support your organization over the whole migration process. Feel free to contact us for further information.

Introduction

Quantum computing will benefit the entire world

The promises of quantum computing are phenomenal. Some concrete examples of the positive impacts include:

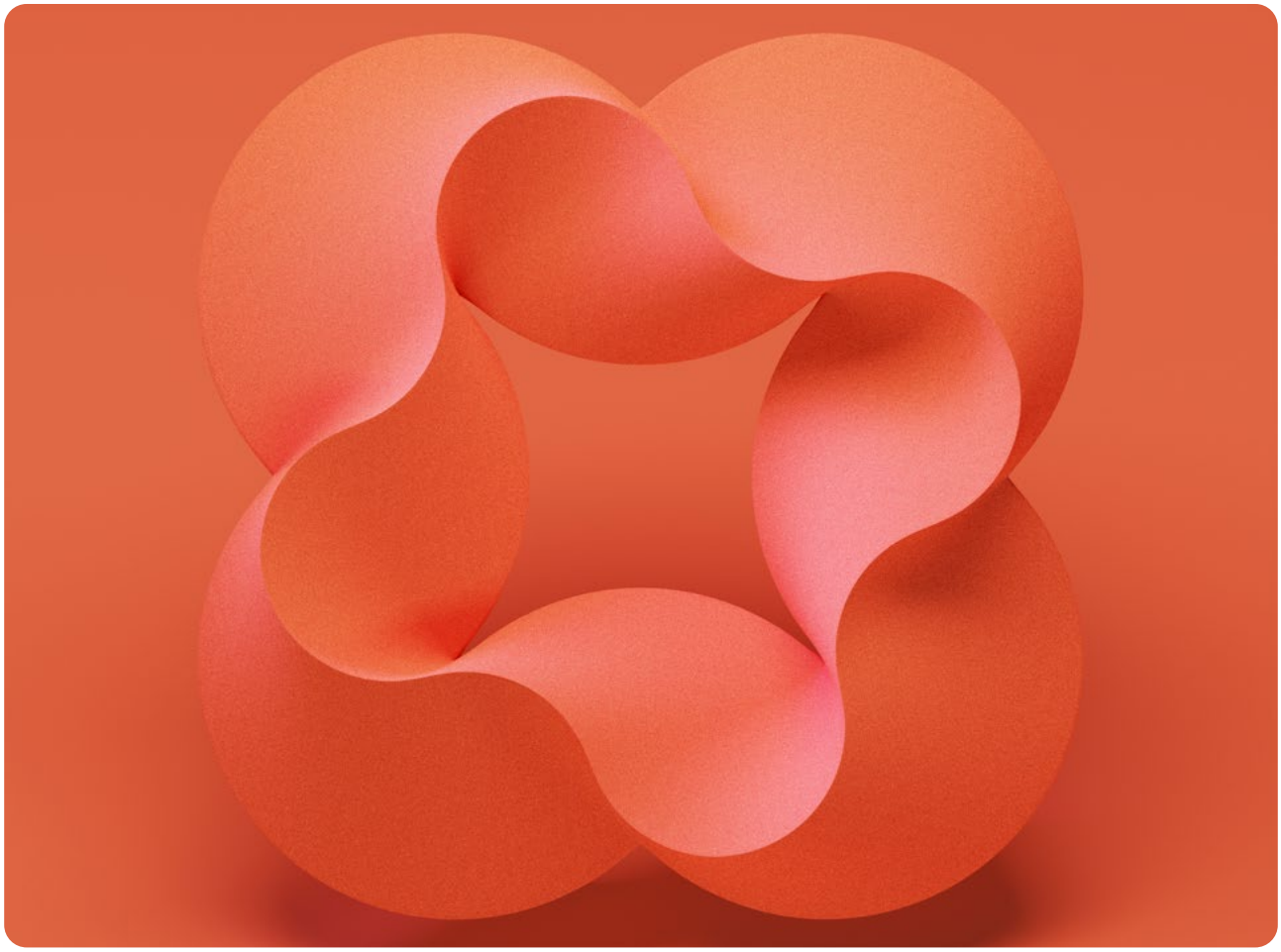
- Quantum computers can contribute to progress in low-carbon technologies by revolutionizing chemistry, helping humanity to contain global warming[1];
- Quantum computers can solve real-world issues in drug discovery and preclinical drug development[2];
- Quantum computers can unlock the potential of safe autonomous driving vehicles[3];
- Quantum computers will dramatically speed up and extend the capabilities of artificial intelligence[4],

Additional applications of quantum mechanics include quantum random number generation (QRNG), quantum key distribution (QKD), and quantum sensors used for radar, geo-positioning, brain imaging, and particle detection.

Did you know that Eviden:

- developed a Quantum Learning Machine QLM;
- can help you adopt the Quantum technology;
- developed Q-score, a new quantum metrics reference;
- offers myQLM, a python package.

Learn more in “What Eviden can do for you” at the end of document.



1. https://www.weforum.org/agenda/2019/12/quantum-computing-applications-climate-change/
2. https://pharmafeatures.com/drug-discovery-quantum-computing/
3. https://www.newsweek.com/ibm-using-quantum-computing-help-automotive-industry-solve-ev-traffic-problems-1637827
4. https://www.researchgate.net/profile/V-Moret-Bonillo/publication/265642441_Can_artificial_intelligence_benefit_from_quantum_computing/links/54f0b8090cf2b36214aae3a2/Can-artificial-intelligence-benefit-from-quantum-computing.pdf

What are the threats to cryptography?

As we've explained in our "Introduction to post-quantum cryptography" whitepaper[5], there are serious threat posed by quantum computers.

Imagine that a hacker is capable to penetrate almost any corporate network or connect to the same private network as your employees and spy on it. Assume that the same hacker can read all en¬crypted emails and network communications that they encounter, as if they plain text. Finally, imagine that this threat actor can hijack every protected WWW and VPN connection within reach.

Unfortunately, these scenarios are not science fiction as nearby on the computing horizon there will be quantum computers that will be capable of factorizing large prime number products. In this paper we will qualify such quantum computers as "cryptographically relevant quantum computers". Devices of this kind could be used to crack several important cryptographic algorithms, including RSA and Diffie-Hell¬man, two systems that are used billi¬ons of times in web browsers, connected objects, e-mail clients, smart¬phones, ATMs, etc. A dystopian digital apocalypse would become reality.

Fortunately, we're not there yet. Although quantum computers already exist, current models can at most decompose two-digit num¬bers into their factors. To threa¬ten current asymmetric systems such as RSA or Diffie-Hellman, they would have to manage a similar operation with a 700-digit num¬ber. This not be feasible to do today or tomorrow.

Nevertheless, numerous organizations are currently conducting intensive research on quantum com¬puters which results in constant performance improvements. This brings us closer to both the benefits of this technology but also draws us closer to the brink of compromising de facto cryptographic methods. Therefore, it is imperative to research viable alternatives to RSA, Diffie-Hellman and a other systems that may not be readily vulnerable to cryptographically relevant quantum computers. Fortunately new methods already exist, and they are grouped under the term post-quantum cryptography.

So far, post-quantum cryptogra¬phy methods are seldom used in practice. further there is not a large historical research base to draw from. However, significant progress is being made as and several post-quantum methods have recently emerged as viable alternatives with which we can venture into a new epoch **post-quantum cryptography.**

This guide focuses on the migration path to post-quantum cryptography. It outlines the major challenges of ensuring your corporate IT environment quantum-resistant and how illustrates how these challenges can be solved. Moreover, it will show what Eviden can do for your enterprise or your authority in order to enable a smooth transition to the post-quantum world.

Standardization

In 2017, the US National Institute of Standards and Technology authority (NIST) launched a competition pitting post-quantum cryptographic methods against each other. Experts from all over the world were invited to submit suitable algorithms to a selection process where the best methods would be identified and proposed for use. This competition included both signature algorithms and encryption/key-exchange methods. The final result was to be a portfolio of reliable post-quantum methods suitable for different purposes based on diverse mathematical foundations.

NIST admitted 69 of the submitted methods into the competition. In July 2022, after three rounds of evaluation, four winners were announced: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+. The two CRYSTALS methods are expected to become the preferred algorithms for the next decades with CRYSTALS-Kyber used for key exchange and CRYSTALS-Dilithium for digital signatures.

The NIST jury also identified four additional candidates (later reduced to three, as one algorithm proved unsecure) for further analysis and evaluation in a fourth round. Finally, NIST announced a new competition for signature methods suited for short and quickly verifiable signatures

It is anticipated that these winning algorithms will be incorporated in numerous standards and products worldwide. For instance, the German Federal Office for Information Security (BSI) and the French IT security agency (ANSSI) are expected to adapt their recommendations and regulations accordingly.

The Internet Engineering Task Force (IETF), the Internet's standardization body, will likely take cues from the NIST competition. Independently, the IETF has published two "Requests for Comments" (RFCs) specifying post-quantum procedures that didn't take part in the NIST competition, namely the signature schemes XMSS (RFC 8391)[6] and Leighton-Micali (RFC 8554)[7].

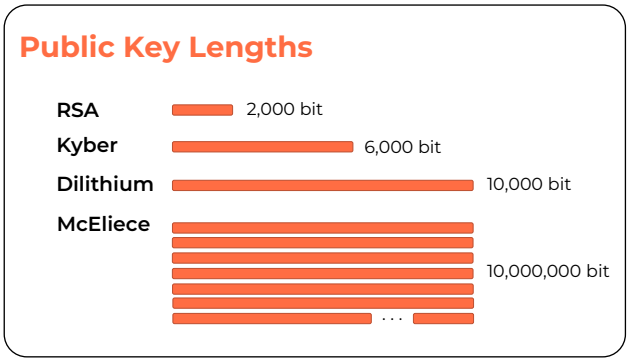


Figure 1: The public keys of post-quantum algorithms are much longer than the ones of conventional systems such as RSA.

The road to a post-quantum world

Accurate prediction timelines when quantum computers capability to break real cryptosystems remains elusive, so assumptions have to be made. The National Security Agency (NSA), the United States' cybersecurity authority, mandates that the owners and operators of national security systems to start using post-quantum algorithms no later than 2035[8]. The German BSI operates on the working hypothesis that pre-quantum crypto methods will become insecure in the early 2030's.[9]

All currently available post-quantum methods differ from RSA and Diffie-Hellman in major aspect. Most significantly, the keys of post-quantum algorithms are often considerably longer than the keys of conventional schemes. For instance, the public keys of CRYSTALS-Kyber (6,000 bit) and CRYSTALS-Dilithium (10,000 bit) are several times larger than the ones of RSA and Diffie-Hellman (2,000 bit). Other proposed post-quantum algorithms even require hundreds of thousands of public-key bits more. The situation is not much different when it comes to private keys. Despite the novel methods, post-quantum encryption/decryption, key generation, signing and verification operations are frequently less performant than those of the status quo[10].

Most experts recommend hybrid cryptographic mechanisms for a transition phase. A hybrid cryptographic mechanism combines a recognized pre-quantum public key algorithm and a post-quantum method, so that an attacker needs to break both of these to be successful. Schemes of this kind enable backwards compatibility while preventing potential weaknesses in post-quantum algorithms resulting in security threats.

Several hybrid cryptographic network protocols are currently being standardized, e.g. PCQ variants of TLS and IKEv2. Public Key Infrastructures (PKI), including the formats of digital certificates, are likewise being adapted,

Unfortunately, there lacks consensus regarding hybrid mechanisms which may prove confusing.[11] While the German BSI and the French ANSSI clearly recommend the implementation of this approach, other IT security authorities advise against it. The EU organizations ETSI and ENISA allow the use of these options, but they don't state a recommendation for or against it. Hopefully, additional analysis will lead to eventual agreement amongst the experts.

As a design principle, it is desirable for the encryption methods used within an IT architecture system to be interchangeable. This paradigm is known as **crypto-agility.** In order to be crypto-agile, manufacturers of cryptographic software are expected to enable selection from a suite of preferred cryptographic algorithms while simplifying the additional procedures needed to change to an alternative. The ability to react quickly by pivoting from a compromised method to a secure mechanism will be of paramount importance.

> **"As cryptography is used in considerable amounts of assets and infrastructure, moving from one cryptographic algorithm to another is a big undertaking."**
>
> Anna Katharina Lindner, M.Sc. Siemens

The use of post-quantum cryptography is thus inextricably linked to the crypto-agility paradigm. Undoubtedly, consumer demand will drive crypto-agile development and manufacturers will strive to meet this shift in focus. Standards, benchmarks, and certifications all will evolve. We believe that, like the US Executive Order **"H.R.7535 - Quantum Computing Cybersecurity Preparedness Act"**, several countries will adopt regulations to push their sensitive industries to prepare and execute a migration plan.

Figure 2: Crypto agility requires that cryptographic algorithms can be changed easily.

5. https://atos.net/wp-content/uploads/2022/11/Atos-cybersecurity-cryptovision-Post-Quantum-Whitepaper-EN.pdf
6. https://www.rfc-editor.org/rfc/rfc8391
7. https://www.rfc-editor.org/rfc/rfc8554.html
8. https://fedscoop.com/nsa-sets-2035-deadline-for-adoption-of-post-quantum-cryptography-across-natsec-systems/
9. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf
10. https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study
11. https://pkic.org/events/2023/post-quantum-cryptography-conference/pkic-pqcc-pqc-at-ietf-mike-ounsworth-entrust.pdf

Migration to post-quantum crypto systems

General

Now that new standards are within reach and crypto vendors are adapting their products, it is time for enterprises and authorities to occupy themselves with post-quantum cryptography as well. The current outlook dictates migrations to PQC methods within the next ten years. A phased project that dealing with these tasks should be planned. Considering that large organizations typically uses dozens, if not hundreds, of crypto applications, this represents a significant undertaking.

It is important to note that not all cryptographic implementations are affected by cryptographically relevant quantum computers in the same way. Symmetric methods, such as AES and Triple-DES, do not need to be replaced by new cryptographic systems. Instead, it is sufficient to use these ciphers with appropriate key lengths. 256-bit lengths are expected to withstand even the most powerful cryptographically relevant quantum computers. In many cases, 256 bit keys are already in use and where not used, many hardware and software systems already allow for an easy key length change. However, when AES and Triple-DES are used in hybrid from with RSA they vulnerable regardless of key size.

On the other hand, implementations using RSA, Diffie-Hellman and other current asymmetric systems will eventually be discontinued and replaced by quantum-proof algorithms. This is also true for other crypto systems based on factorization, including Fiat-Shamir, those on discrete logarithms, including DSAm and systems using elliptic curves (ECC) are not quantum-proof and require replacement.

As not all applications of asymmetric cryptography can be attacked the same way, the following distinctions should be made:

1. Encryption and key exchange: Asymmetric algorithms used for this purpose can be attacked at the time they of use, but also later. For instance, an attacker may try to decipher an encrypted email that was sent years earlier **(store now, break later)**. Because of this threat, the transition to post-quantum encryption should be made as soon as possible.

2. Data signatures: Signed payload data may be subject to a "store now, break later" attack also. For example, an attacker might want to tamper with signed information that was created years earlier. This means that signature systems used for payload data need to be replaced in time as well.

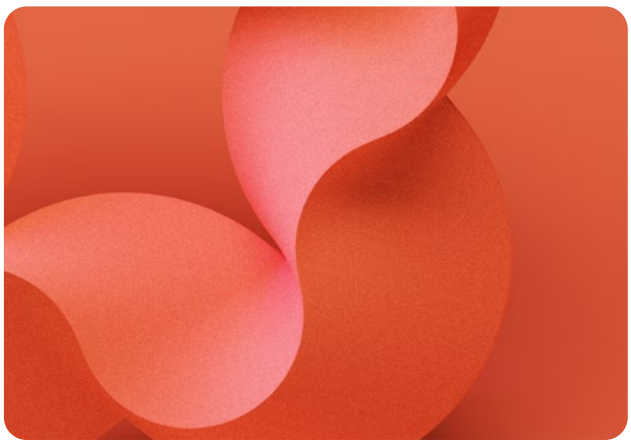
3. Authentication signatures: Signatures used for authentication, as utilized by transport-layer protocols such as TLS and IKE, are verified immediately. If the signature is correct, the signer is granted access, otherwise it is rejected. Signatures of this kind have no value at a later stage. For this reason, the transition of authentication signature schemes is less time-critical than mentioned previously.

It is evident that replacing asymmetric encryption, key-exchange, and data-signature algorithms alone is not sufficient to prevent "store now, break later" attacks. Additional measures for preexisting encrypted or signed data need will need re-encryption and signed again with post-quantum methods.

As mentioned above, some experts recommend a hybrid mechanism for a transition phase. If you follow this advice, your IT systems not only must be made post-quantum ready, but also be prepared for hybrid mechanisms. In many cases, this will prove to be challenging as it is often easier switching algorithms than introducing support of several algorithms at the same time.

Migration to post-quantum cryptography will become easier when the crypto technology used in an organization meets these requirements:[12]

- The operator understands any regulatory compliance requirements.
- The operator has an inventory of crypto is used and where.
- A Certificate Lifecyle Management (CLM) system is implemented.
- A Key Management System (KMS) is used.
- Crypto algorithms are not hard-coded or applications are crypto-agile.
- The operator is prepared to use algorithms that are slower and use longer keys.
- Crypto libraries are kept up to date, software that is no longer supported is phased out.



12. Paul van Brouwershaven, Chair of the PKI Consortium, during the March 2023 PQC Conference

Steps of the migration process

Migration to post-quantum cryptography in your organization should follow a structured approach. The ETSI report on migration strategies[13] recommends steps for such a project. In alignment with this guidance, Eviden has developed detailed migration scheme. This business- and practice-oriented process consists of six key steps:

1. Project setup
2. Crypto inventory creation
3. Understanding of your risks
4. Organization and policies impact assessment
5. Executive sponsorship buy-in
6. Migration execution

Why we should hurry

- Possible quantum technology breakthrough
- Migrating will be long and complex
- Some data need long-term protection
- Attackers are storing data now to decrypt it later

... carefully

- No standards yet
- Network protocols are not ready yet
- Migration will be hard
- Lack of skills
- Interoperability challenges
- No security certification available yet

Figure 3: Migration to post-quantum cryptography is a challenge.

Project setup

At the beginning, your organization needs to perform an initial business risk analysis which is presented to the executive team in order to secure attention and approval. This risk assessment would typically include the impact and damage potential of encrypted data leakage being compromised by quantum-vulnerable components or unexpected downtime and a compliance breach due to reliance on legacy algorithms. This step may also preliminary budgetary considerations. If the project setup decision is approved, a larger migration project will be assessed, organized, and planned.

Did you know that Eviden Strategic Cybersecurity Advisory teams have developed a methodology for this "first level business risk analysis"?

Learn more in "What Eviden can do for you" at the end of document.

13. https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

> “Now is not the time to panic, it is the time to plan”

Troy Lange (NSA) at ICMC 2022

Crypto inventory creation

Before the actual migration to post-quantum cryptography can take place, it is essential to know where cryptography is used within the organization. Determining the full scope of crypto enable applications or infrastructure components can be daunting. Typical applications using cryptography plentiful and include PC operating systems, web-browsers, VPN solutions, IP telephony smartphone apps and a myriad of others. In many cases, users are not even aware of that cryptography is being utilized.

To address this challenge, a catalog of all cryptographic applications and infrastructure components needs to be compiled. This **crypto inventory** will contain concise information about each component using cryptography including:

- Vendor
- Is it a hardware or software solution?
- Where is the component used
- Cryptographic algorithms used (asymmetric and symmetric, although the latter are less exposed)
- Keys and key stores
- Digital certificates
- Protocols
- Cryptographic providers and libraries

In addition, a crypto inventory should detail infrastructure components, such as a Public Key Infrastructure (PKI) and links to certificate policies and practice statements.

The level of detail that each assets record in a crypto inventory must observe should strike a clear balance between full exhaustivity and the capacity to start the migration in time. Operational constraints may warrant a continuous improvement approach that includes updating or adding new information to the inventory over time when applied.

Eviden and their partners provide tooling that support the generation and maintenance of a crypto inventory. Despite the automation potential, some tasks may still have to be done by hand as they require institutional knowledge and understanding of IT and business aspects of an organization. Identifying the components that use cryptography and its function within infrastructure may not be readily available to inventory scans and could be overlooked.

As not all assets might be discovered at once, the crypto inventory discovery and update should be a continuous process in the organization and never be stopped. Additionally, every new application project (business driven) has the potential to change the crypto inventory by starting or stopping to use cryptography, changing its infrastructure layers or modifying its risk profile.

Did you know that Eviden Strategic Cybersecurity Advisory teams have developed a methodology to help you create, maintain, and continuously improve your crypto inventory ?

Learn more in "What Eviden can do for you" at the end of document.

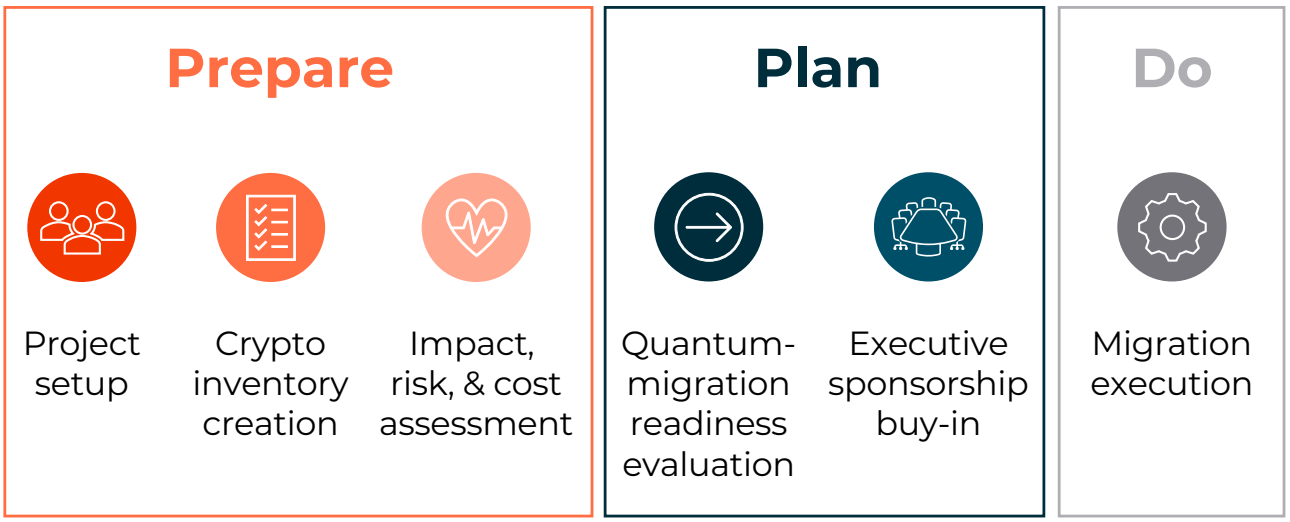


Figure 4: The Eviden post-quantum-migration scheme

Quantum-migration readiness evaluation

Migrating applications listed in the crypto inventory will have varying degrees difficulty. To produce a meaningful overview, it is recommended that systems be classified according to the **quantum migration readiness evaluation** scheme:

1. PQC-ready: The application already supports (asymmetric) post-quantum methods or sufficient (symmetric) key lengths.
2. Crypto-agile: The application is not PQC-ready but is designed to support crypto-agility.
3. PQC readiness plan: The application is not crypto-agile but the vendor has a PQC readiness plan.
4. Readiness option: There is no PQC readiness plan for this application yet, but there is potential for one in the near future.
5. No readiness option: The application might never be PQC ready.

Since creating a crypto inventory and assessing it according to different criteria is a comprehensive task it is recommended to have such a catalog checked assessed by a third party. It widely expected that external validation of quantum migration readiness evaluation strategies will become a standard procedure. It is highly likely these audits will be required by legal regulations and governed by evaluation standards. Standardized evaluation schemes and certificates for the successful implementation may evolve. However, these developments are still in their infancies.

Impact, risk, and cost assessment

In this step, every entry of a crypto inventory must be assessed with respect to its impact on the organization and the risk associated if it isn't made quantum-resistant in time.

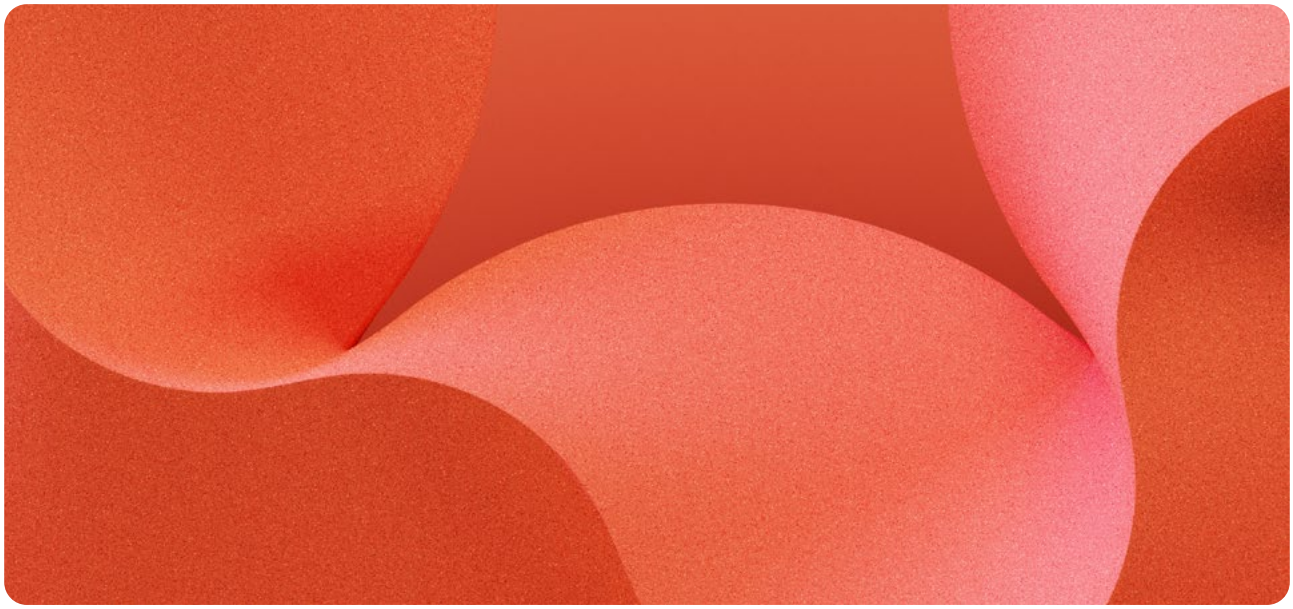
Impact considerations should include the a review of contracts and ideally contracts should include a mention if a solution is, or must be, made quantum-ready.

Risk assessments consists of two parts. First, the probability of for each system being attacked needs to be estimated. For instance, an encrypted wireless network connection is much easier to attack than an encrypted document stored on a file server equipped with the standard security mechanisms.

Of course, using post-quantum cryptography is not without risk. Switching to post-quantum algorithms might lead to incompatibilities and result in unexpected downtime and service interruption. Additionally, migration risks of invalid implementation must be taken into account. Finally, because PQC methods are not as mature or as exhaustively researched as the legacy mechanisms, risk of a vulnerability these novel methods also needs to be accounted for.

The second part of the risk-assessment quantifies the potential damage caused by an attack. This means that the costs incurred due to a security incident based on non-quantum-proof legacy systems must be estimated.

Finally, the post-quantum migration project plan should be planned and the costs estimated. This may include expanding and training the staff, as well as, contracting consultants. Experts predict that there will be significant demand for skilled cybersecurity staff who are capable of managing the migration meaning their rates will come at a premium.



Executive sponsorship and buy-in

After having completed the previous steps, it is necessary to reinvolve the management of your organization. At this juncture you will need to explain them why post-quantum migration is necessary and the risks if this process is delayed. In addition, you need to provide a budget planning for the migration project. After evaluating this information the management board will be well prepared to decide how to proceed with the migration project.

Migration execution

Now that the challenges and risks of post-quantum migration are understood, the project planned and budgeted, execution can finally begin. Since it is impossible to perform all replacements at once, prioritization is necessary.

Typically, organizations target the infrastructure with critical priority. This is especially true for PKI, because standardized post-quantum algorithms will need to be deployed first before any certificate- based application can be made post-quantum ready.

The schedule for the replacement must be administered based on the following criteria:

- State of the art of quantum computers: Currently, it seems unrealistic that quantum computers capable of breaking current crypto systems will become available before 2030[14]. However, advances in this technology should be monitored and, if necessary, the migration process should be accelerated.
- State of the art of post-quantum cryptography: Although post-quantum cryptography has made considerable progress in recent years, there will be new developments. For example, none of the three electronic signature algorithms chosen by the NIST solves all issues, and therefore new ones are being designed. With the advent of new methods, the project plan might have to be amended.
- Dependence from infrastructure: Some crypto solutions rely on a user management or procurement systems. Asymmetric crypto systems usually use digital certificates provided by a PKI. It evident that components can only be updated if the infrastructure it relies has been migrated. Conversely, stand-alone systems, such as a component using symmetric cryptography without external key management, can be addressed independent of the readiness of the infrastructure.
- PQC readiness: Of course, only PQC ready components can be migrated.
- Risk: Components with a high risk of being attacked or with a high damage potential are prioritized. The riskiest items should be migrated first, then followed by less critical components.

Resources required for the actual migration need to be planned. Staff must be provided and trained.

Ongoing managing migration projects should also include monitoring the current state of quantum computer technology and the PQC readiness of the systems in the crypto inventory. Ideally, crypto inventory will be updated during the migration, as well as when new applications are introduced in the company.

As such, every new addition to the crypto inventory (as not all assets might have been discovered at once), should lead to restarting, as a continuous cycle, steps 3 to 6 (understand risk, org and policies assessment, exec sponsorship and migration execution) for the newly added scope.

14. https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

Understanding post-quantum cryptography

Eviden is aware that post-quantum cryptography will only be realized when specialists, developers, consultants, IT managers, administrators, and IT executives all come to grips with it. This represents a significant learning curve and long adoption timeline which leads to a challenging situation, as the math behind post-quantum cryptography is complex and differs significantly from the principles that have prevailed in cryptography to date. For instance, understanding CRYSTALS-Kyber and CRYSTALS-Dilithium is more difficult than comprehending systems like RSA and Diffie-Hellman.

Because this degree of crypto literacy is not widely prevalent, Eviden is actively involved in many activities that aim to help explain post-quantum cryptography to non-mathematicians in many diverse ways.

One of the explanatory models developed by Eviden is based on cartoons and everyday analogies (see Figure 2) and is distinctive worldwide. These comic illustrations have been published in whitepapers and magazine articles and are presented with audience acclaim at leading security events across the globe.

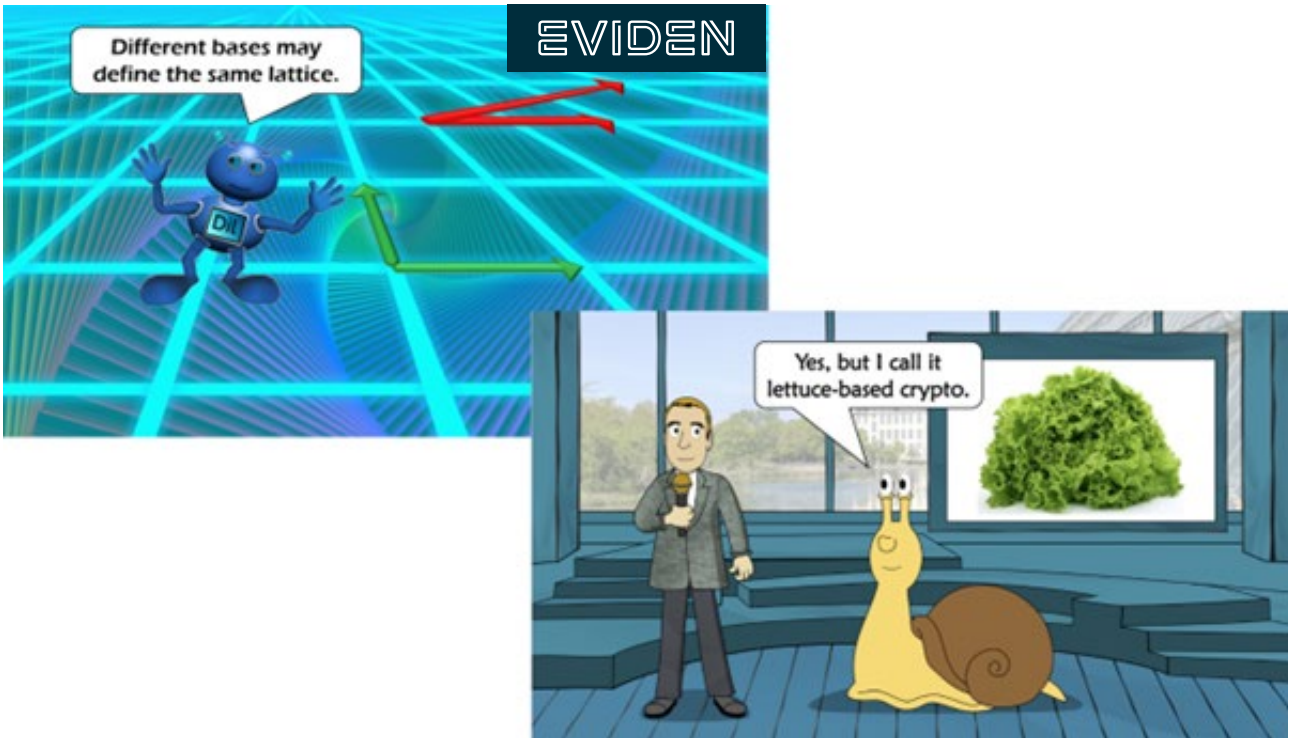


Figure 5: Eviden PQC-cryptography concepts illustrated for non-mathematicians.

What Eviden can do for you

Eviden helps its customers grasp the benefits that quantum computing brings to their business, and also helps them to anticipate the threats it creates, by preparing and planning their post-quantum cryptography migration.

On the one hand, quantum computing comes with phenomenal promises which will help tackle challenges too complex for classical computers. Eviden helps its customers explore and prepare for this future of quantum computing through proven methodology and leveraging its Quantum Computing assets, notably:

- The **Eviden Quantum Learning Machine** QLM, a complete programming development platform and the **highest-performance quantum simulator in the world.** Eviden QLM is used in numerous countries empowering research programs in various sectors.
- We provide consulting and innovation services to **understand, evaluate, identify real use cases, and adopt the technology.** We are the only player in the field of quantum hybridization, the convergence of high-performance computing (HPC) and quantum computing.
- We developed Q-score, a new **quantum metrics reference,** applicable to all quantum processors. It measures the efficiency of running a representative quantum application, a system's effectiveness at handling real-life problems, instead of its theoretical or physical performance.
- We offer **myQLM, a python package** that is provided with open-source interoperability connectors.

On the other hand, cryptographically relevant quantum computers have the potential to break the existing asymmetric cryptography standards.

Eviden has taken the challenge to raise their customers' and the public's awareness by presenting the topic at Cybersecurity and other industries events and through several publications:

- An analysis on using hybrid cryptosystems by combining a classical algorithm with a post-quantum algorithm
- A comprehensive yet generally accessible **"Introduction to post-quantum cryptography" whitepaper.**

Eviden Strategic Cybersecurity Advisory teams developed methodologies for customers to:

- Develop their "first level business risk analysis" aiming at assessing the extent of the program,
- Create, maintain, and continuously improve their crypto inventory,
- Assess their pre-quantum cryptography risks, with their probability and impact,

Eviden applies the approach and methodologies throughout its own organization. The migration of its cybersecurity products is ongoing, with PQC readiness plans and detailed roadmaps communicated to the customers requesting them

- Hardware Security Modules **(Trustway HSM)**: powerful general purpose Hardware Security Module appliances, Common Criteria EAL4+ certified, Reinforced Qualification (ANSSI QR), EU restricted and NATO secret, amongst other certifications, used for highly secured generation and management of encryption keys as well as processing cryptographic operations. They will integrate PQC selected signature schemes by Q4 2023 (Crystals-Dilithium, Falcon and Sphincs+).

In a nutshell:

- Public Key Infrastructure **(IDnomic PKI)**: a powerful, multi-purpose Public Key Infrastructure software suite for production and issuance of trusted digital identities, compliant to highest security standards. The product is crypto-agile in design capable of issuing hybrid certificates for legacy and PQC ready applications enabling a smooth migration path for its users.
- Email and file encryption **(Cryptovision Greenshield)**: solution approved for the exchange of classified information (EU and NATO restricted, German VS-NfD) accredited by the German BSI and the EU-Council. The product's architecture is modular and flexible based on crypto-agile development. With its PQC-readiness it allows seamless usage of traditional algorithms as well as future quantum resistant ones.
- Identity and Access Management **(Evidian IAM)** a suite of products protecting companies from attacks by unauthorized users. Usage of cryptographic primitives, algorithms, and protocols, will comply with the upcoming iterations of standards such as SAML, OIDC and OAuth 2, and more specifically their usage of security mechanisms such as XML Encryption and Signature, along with JWT signature for ID and Access tokens. These will embrace the new post-quantum cryptography standards, such as currently defined by the NIST.

Within its Cybersecurity product range, Eviden has placed great emphasis on facilitating crypto inventories and crypto-agility.

Our products typically support multiple cryptographic methods for the same purpose with the ability to switch between them at the click of a mouse.

Eviden is involved in several European research and development projects, like experimenting the pragmatic use of post-quantum cryptography within PKI smartcards.

Conclusion

Eviden is an expert in the fields of quantum computing and cryptography and based on this unique combination your ideal partner in the context of post-quantum cryptography. Their cryptography products, including HSMs, email encryption software, VPN solutions, and PKI systems, are currently made quantum-proof. In addition, Eviden supports your organization in the migration process. Feel free to contact us for further information.

For more information, please contact: **cybersecurity@atos.net**

Connect with us

eviden.com